⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2−116924

⑤Int.Cl.⁵	識別記号	庁内整理番号
G 06 F 3/06	304 H	6711−5B
3/08	F	6711−5B
12/14	320 C	7737−5B

⑬公開　平成2年(1990)5月1日

審査請求　未請求　請求項の数 10　(全8頁)

⑤④発明の名称　データ秘密保護方式

⑳特　願　昭63−269376

㉒出　願　昭63(1988)10月27日

⑦②発明者　園部　武雄　大阪府茨木市丑寅1丁目1番88号　日立マクセル株式会社内

⑦②発明者　山内　暁　大阪府茨木市丑寅1丁目1番88号　日立マクセル株式会社内

⑦①出願人　日立マクセル株式会社　大阪府茨木市丑寅1丁目1番88号

⑦④代理人　弁理士　武　顕次郎　外1名

明　細　書

1．発明の名称

データ秘密保護方式

2．特許請求の範囲

(1)　光記録媒体に記録されているデータの秘密保護方式において、該光記録媒体に特定のフォーマットで該データが記録されているとともに、少なくとも1つの情報参照エリアが設けられて該情報参照エリアに該光記録媒体を使用するユーザ固有の情報が記録されており、該特定のフォーマットについてデータ再生を行なうシステムに外部から入力される比較情報と該光記録媒体から読み出された該ユーザ固有の情報とを比較し、両者が一致したときのみ該システムは該光記録媒体から該データの再生を可能としたことを特徴とするデータ秘密保護方式。

(2)　請求項(1)において、前記比較情報と前記ユーザ固有の情報との比較処理手段を前記光記録媒体のドライブ装置に設けたことを特徴とするデータ秘密保護方式。

(3)　請求項(1)または(2)において、前記ユーザ固有の情報は、筆跡、指紋、印章、声紋、顔写真、眼底模様などの情報の少なくとも1つであることを特徴とするデータ秘密保護方式。

(4)　請求項(1)、(2)または(3)において、前記光記録媒体は秘密保護を必要とするユーザデータが記録されたユーザデータエリアと該ユーザデータ夫々に対するデイレクトリデータが記録されたデイレクトリデータエリアとを有し、前記ユーザ固有の情報と前記比較情報とが不一致のときに該デイレクトリデータエリアに記録されている該デイレクトリデータの再生を不能とすることを特徴とするデータ秘密保護方式。

(5)　請求項(4)において、前記デイレクトリデータエリアに記録されているアドレスデータを所定個数おきに破壊して前記デイレクトリデータの再生を不能とすることを特徴とするデータ秘密保護方式。

(6)　請求項(5)において、破壊されないアドレスデータからのアドレス部検出回数により；破壊され

た前記アドレスデータの検出を可能としたことを特徴とするデータ秘密保護方式。

(7) 請求項(1)、(2)または(3)において、前記光記録媒体は秘密保護を必要とするユーザデータが記録されたユーザデータエリアと該ユーザデータ夫々に対するディレクトリデータが記録されたディレクトリデータエリアとを有し、前記ユーザ固有の情報と前記比較情報とが不一致のときに該ディレクトリデータエリアに記録されている該ディレクトリデータを判読不能とすることを特徴とするデータ秘密保護方式。

(8) 請求項(7)において、前記ディレクトリデータに所定パターン情報を重ね書きして前記ディレクトリデータを変調し、前記ディレクトリデータを判読不能とすることを特徴とするデータ秘密保護方式。

(9) 請求項(8)において、前記変調されたディレクトリデータは所定の復調コードで復調可能とすることを特徴とするデータ秘密保護方式。

(10) 請求項(7)において、前記ディレクトリデータを判読不能とするためのプログラムを前記光記録媒体の特定エリアに記録したことを特徴とするデータ秘密保護方式。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は、光記録媒体や磁気記録媒体などに記録されているデータの管理方式に関する。

〔従来の技術〕

光ディスク、磁気ディスクなどの大容量の記録媒体を用いたシステムとして、多数の必要なデータを記録媒体に記録して管理するデータファイルシステムが知られているが、このデータファイルシステムも種々の分野に利用されるようになり、たとえば個人的データのように、決められた者しか利用できないデータの管理にも利用されるようになつてきている。この個人的データを管理するシステムの一例としては、たとえば、医療用のデータの管理システムがあり、個人のX線写真などをファイルするものであつて、他人に対しては秘密性を保持する必要がある。

一方、個人的データの秘密性を保持するデータファイルシステムとしては、従来、ＩＣカードシステムが知られている。これはマイクロコンピュータとメモリとを内蔵するＩＣカードを用いるものであつて、メモリに必要なデータが記憶されているとともにマイクロコンピュータに暗証番号が格納されており、外部から入力される暗証番号がマイクロコンピュータに格納されている暗証番号と一致したときのみ、マイクロコンピュータがメモリからのデータの読出しを可能とするものである。

〔発明が解決しようとする課題〕

上記のＩＣカードシステムでは、上記のように暗証番号の一致、不一致によつてＩＣカード内のマイクロコンピュータがメモリからのデータ読出しの可、不可を決定するものであるから、メモリの記憶されているデータに対して高い秘密性を維持できる。つまり、メモリからのデータ読出し手段であるマイクロコンピュータがこのメモリとともにＩＣカードに内蔵され、しかも暗証番号によつてのみ動作するものであり、これ以外の手段ではマイクロコンピュータが動作しないから、データの秘密性を維持できるのである。

これに対し、光ディスクや磁気ディスクなどの記録媒体はデータが記録されているだけのものであり、ドライブ装置に取りつけることによつて容易にデータの読み出しが可能である。ＩＣカードシステムと対比して暗証番号によりドライブ装置による記録媒体からのデータ読出しの可、不可を決定するようにすることも考えられるが、これは特定のドライブ装置について可能であつて、暗証番号を必要としない他のドライブ装置や既存のドライブ装置を用いれば簡単にデータ読出しが行なえる。

以上のように、光ディスクや磁気ディスクなどを用いたファイルシステムでは、従来、データの秘密性を保持することは不可能であつた。

本発明の目的は、かかる問題点を解消し、記録媒体に記録されているデータの秘密保護を実現可能としたデータ秘密保護方式を提供することにあ

る。

〔課題を解決するための手段〕

上記目的を達成するために、本発明は、記録媒体のデータフォーマットを特定化するとともに、該記録媒体に少なくとも1つの情報参照エリアが設けられて該情報参照エリアにユーザ固有の情報が記録されており、該特定のフォーマット化された該記録媒体のデータ再生を行なうシステムで外部から入力される比較情報と該記録媒体から読み出された該ユーザ固有の情報とを比較し、両者が一致したときのみ該システムは該記録媒体から該データの再生を可能とする。

また、本発明は、記録媒体がユーザデータエリアとディレクトリデータエリアとを有し、前記ユーザ固有の情報と前記比較情報とが不一致のとき、該ディレクトリデータエリアからのディレクトリデータの再生を不能、もしくは該ディレクトリデータエリアから再生されるディレクトリデータの判読を不能とする。

〔作用〕

記録媒体に記録されているデータは特定のフォーマット化されているために、この特定のフォーマットを取り扱うドライブ装置でしかデータ再生ができない。これにより、データ再生が可能なドライブ装置が特定される。しかも、データ再生が可能なドライブ装置に該記録媒体を使用しても、入力される比較情報が該記録媒体に記録されているユーザ固有の情報と一致しなければ、該記録媒体からのデータ再生は行なわれない。該ユーザ固有の情報としては指紋，筆跡や印章などの情報を用いることができ、個人個人の判別が可能となる。したがつて、データの秘密保護が完全に達成されることになる。

また、ユーザ固有の情報と比較情報とが一致しないとき、ディレクトリデータの再生や判読が不能となるようにすることにより、該記録媒体が不正使用された痕跡を残すことができるし、また、さらに確実に不正使用に際してのデータ再生を防止することができる。

〔実施例〕

以下、本発明の実施例を図面によつて説明する。

第1図は本発明によるデータ秘密保護方式の一実施例を示すブロック図であつて、1はホストコンピュータ、2はディスクドライブ装置、21，22は画像バツファ、3は光ディスク、4はイメージスキヤナ、5はディスプレイ装置である。

同図において、光ディスク3は、たとえばISO－9171で規格されたカートリツジ付きの5.25インチ光ディスクであつて、ユーザデータエリアとディレクトリデータエリアとを有している。ユーザデータエリアには、たとえばX線写真などの秘密保護が必要な画像データが多数記録されており、ディレクトリデータエリアには、各画像データについて、スタートアドレス、データ長、ファイル名、日付などのディレクトリデータが記録されている。ここで、これら画像データ、ディレクトリデータは特定のフォーマットで記録されており、さらに、光ディスク3には、これらユーザデータエリア、ディレクトリデータエリアとは異なる特定のエリア（以下、これを情報参照エリアという）に、この光ディスク3の所有者などのユーザ個人を表わす特定の情報（以下、これをユーザ固有情報という）が記録されている。このユーザ固有情報としては、指紋、眼底模様、顔写真などの身体的特徴を表わす情報、筆跡、声紋などのユーザから生ずる特徴を表わす情報、印章などのユーザの所有物の特徴を表わす情報などが用いられる。数値のパターンからなる暗証番号であつてもよい。

イメージスキヤナ4は、かかるユーザ固有情報が指紋などの画像情報である場合には、光ディスク3をディスクドライブ装置2に装着して使用するユーザの指紋などの画像情報の入力手段である。ユーザ固有情報が声紋であれば、入力手段としてマイクロフオンが用いられ、暗証番号であればキーボードが用いられる。以下、かかる入力手段から入力される情報を比較情報と呼ぶことにするが、ここでは、かかる比較情報を画像情報として説明する。

ディスクドライブ装置2には2つの画像バツフ

ア21，22と比較手段（図示せず）とが設けられており、画像バッファ21にはイメージスキャナ4から入力された比較情報がホストコンピュータ1で処理された後格納され、画像バッファ22には光ディスク3から読み出されたユーザ固有情報が格納される。

次に、この実施例の動作を第2図を用いて説明する。

まず、光ディスク3をディスクドライブ装置2に挿入すると（ステップ101）、ホストコンピュータ1はディスクドライブ装置2を起動して光ディスクの情報参照エリアから指紋画像情報であるユーザ固有情報を読み出させる。読み出されたユーザ固有情報はディスクドライブ装置2の画像バッファ22に格納される（ステップ102）。そして、ユーザが必要とする画像データのファイル名を指定するとともに、イメージスキャナ4によつてユーザの比較情報である、たとえば指紋画像情報を入力すると、ホストコンピュータ1はこの比較情報を処理してディスクドライブ装置2に送り、その画像バッファ21に格納させる（ステップ103）。

次いで、ディスクドライブ装置2では、これら比較情報とユーザ固有情報とが比較され（ステップ104）、この比較結果がホストコンピュータ1に送られる。ホストコンピュータ1は、比較情報とユーザ固有情報とが一致したときには、ディスクドライブ装置2にデータ再生指令を送る。これにより、まず、ディスクドライブ装置2は光ディスク3からディレクトリデータエリアの再生を行ない、再生されるディレクトリデータが順次ホストコンピュータ1に供給される。このホストコンピュータ1では、このディレクトリデータでのファイル名とユーザが指示したファイル名とが比較される。両者が一致すると、このファイル名を含むディレクトリデータからスタートアドレスとデータ長を抽出してディスクドライブ装置2に供給し、光ディスク3のユーザデータエリアからユーザが指示したファイル名の画像データの再生を行なわせる。この再生された画像データはホストコンピュータ1でアナログの画像信号に変換され、ディスプレイ装置5に供給される。したがつて、ディスプレイ装置5には、ユーザが希望した画像が表示される（以上、ステップ105）。しかる後、ユーザの指示によつて光ディスク3はディスクドライブ装置2から排出される。（ステップ107）。

ディスクドライブ装置2の画像バッファ21に格納された比較情報と画像バッファ22に格納されたユーザ固有情報とが一致しない場合には、ホストコンピュータ1は光ディスク3からのデータ再生を禁止し、たとえば「ユーザ不適」などのメッセージを出力するエラー処理を行ない（ステップ106）、しかる後、光ディスク3をディスクドライブ装置2から排出する（ステップ107）。

ユーザ固有情報を指紋画像情報としたときの比較については、たとえば昭和63年電子情報通信学会秋季全国大会において、「ICカードの所有者確認のための指紋照合方法」（NEC）と題する論文で発表されている。

以上のように、この実施例では、光ディスク3のデータに特定のフォーマットが使用されていること、比較情報とユーザ固有情報との比較によつて所有者など真のユーザを判定していることから、真のユーザのみがデータ再生が可能となり、光ディスク3に記録されているデータの秘密保持が達成される。

なお、第1図において、画像バッファ21，22や比較手段はホストコンピュータ1などディスクドライブ装置2以外の装置に設けるようにしてもよい。

また、情報参照エリアへのユーザ固有情報の登録処理は、光ディスク3をユーザが購入したときなどで行なわれ、たとえば販売元、あるいはユーザ自身がイメージスキャナ4から指紋などをユーザ固有情報として入力し、ホストコンピュータ1の指示のもとに光ディスク3に記録される。

次に、第3図および第4図により、本発明によるデータ秘密保護方式の他の実施例を説明する。

光ディスクなどの記録媒体では、一般に追記可

能であり、したがつて、不正使用された場合には、記録されている所望データに重ね書きを行なつてこの所望データが変更、もしくは破壊されているような場合もある。このために、光ディスクの記録データの信頼性が低下するという問題もある。特に個人データを記録する記録媒体については、秘密保護とともにデータの信頼性も高める必要がある。この実施例は、第1図に示した実施例についてさらにデータの信頼性を高めるようにしたものである。このために第2図において、比較情報とユーザ固有情報とが不一致の場合、通常光ディスクは不正使用されたことになるので、エラー処理（ステップ106）でその痕跡も光ディスク内に留めるようにする。

第3図はデイレクトリエリアでのセクタフオーマットを示しており、ここでは、"CONTINOUS SERVO OPTICAL 512 BYTE SECTOR FORMAT"に従っている。

第2図のエラー処理（ステップ106）においては、デイレクトリデータエリアにおける1つおきのデイレクトリデータの記録エリアのデイレクトリデータが記録されているセクタに対し、第3図に示す3つの"ID+CRC"ブロックのプリフオーマット化されているトラツクナンバとセクタナンバを表わすアドレスデータを破壊し、このデイレクトリデータが記録されている記録エリアの次のデイレクトリデータが記録されている記録エリアにおいて、この記録エリアの直前の破壊されたアドレスデータを記録する。そして、デイレクトリデータエリア全体についてかかる処理をした後、先の"ユーザ不適"というメツセージを出力する。

このように処理された光ディスクをデイスクドライブ装置に再度挿入した場合には、デイレクトリデータエリアでの上記記録エリアについての判定が不能となるので、デイレクトリデータの再生ができない。これにより、光ディスクが不正使用されたことが判明する。

一方、秘密保護が必要なユーザデータは、一般に、1つの光ディスクにのみ記録され、かつ、いつでも使用できるようにしておく必要がある。このために、上記のようにアドレスデータが破壊された光ディスクはそのまま破棄されるのではなく、他の光ディスクにコピーなどして再利用ができるようにしなければならない。

第4図はこのように破壊処理された光ディスクからユーザデータの再生を可能とするデイスクドライブ装置の一具体例を示すものである。

同図において、デイスクドライブ装置6にはセクタマークカウンタ61とアドレスマークカウンタ62とが設けられている。このデイスクドライブ装置6に第3図に示したように処理された光デイスクを挿入すると、まず、そのデイレクトリデータエリアのデータ再生を行なう。

そこで、いま、アドレスデータが破壊された記録エリアを再生すると、この記録エリアでのセクタ判定は不可能であるが、次の記録エリアでは、アドレスデータが記録されているから各セクタが判定でき、先に説明したように、この記録エリアには、その直前の記録エリアのアドレスデータが記録されているので、これを読み出す。いま、この記録されているアドレスデータが10進数で0010～0016とすると、デイスクドライブ装置6は再度同じトラツクを再生し、このとき、破壊されていない記録エリアから0009のアドレスデータを読み取つたとき、セクタマークカウンタ61とアドレスマークカウンタ62とを夫々0にリセットする。その後、破壊された記録エリアの再生に移るわけであるが、第3図に示す各セクタ毎にセクタマークSMを検出する毎にセクタマークカウンタ62は1ずつカウントアツプし、また、アドレスマークAMを検出する毎にアドレスマーク61は1ずつカウントアツプする。これらのカウント値がセクタのアドレスデータとなるのであるが、いま、セクタマークカウンタ61のカウント値が1でアドレスマークカウンク62のカウント値が3のときには、アドレスデータが0010のセクタと判定される。同様に、セクタマークカウンタ61のカウント値がnで$1 \leq n \leq$

１０のとき、アドレスマークカウンタ６２のカウント値が３ｎであるときには、（００１０＋ｎ）のセクタと判定される。このようにして破壊されたセクタのアドレスデータが復元され、各記録エリアでのディレクトリデータの再生が可能となる。

光ディスクの記録データの信頼性を向上させるための本発明によるデータ秘密保護方式のさらに他の実施例を第５図～第８図により説明する。

この実施例は、ディレクトリデータエリアに記録されているディレクトリデータに変調を施こし、このディレクトリデータの判読を不能にするものである。

すなわち、第２図におけるエラー処理（ステップ１０６）において、光ディスクにおけるディレクトリデータエリアに記録されているディレクトリデータエリアを破壊する。これにより、ユーザデータエリアでの画像データのアドレス指定が不可能になる。他の例としては、記録されているディレクトリデータに特定パターンのデータ（変調データ）を重ね書きしてこのディレクトリデータを変調する。これにより、ディレクトリデータエリアの再生は行なわれるが、ディレクトリデータの判読ができない。この場合、特定パターンの復調データを用いることにより、元のディレクトリデータを復元できるようにする。これにより、ディレクトリデータやユーザデータの他の光ディスクへのコピーが可能となる。

このように、重ね書きによるディレクトリデータの変調および復調処理を第５図～第７図に示す。

いま、ディレクトリデータが２－７変調されているものとすると、第５図において、復調データとして示す元のデータは、夫々変調データとして示すパターンのデータに２－７変調されている。かかるデータに対し、"1" ビットの後に必ず１つ "1" ビットが続くように、重ね書きによる変調を施こすと、第６図に示すように、第５図で変調データであるエラー処理前のデータはエラー処理後のデータとして変換される。かかるデータはもはや２－７変調によるデータではなく、復調不能となつてディレクトリデータは判読不能である。

かかるデータを判読するためには、"0" ビットに続く "1" ビットの次のビットは "0" に変換するという復調を行なうことにより、２－７変調されたデータに変換することができ、これにより、第７図に示すエラー処理後のデータから元の復調データを得ることができ、光ディスクからのデータ再生が可能であつて、他の光ディスクへのコピーが可能となる。

以上のようなディレクトリデータの破壊や重ね書きによる変調処理のプログラム（エラープログラム）はディスクドライブ装置に設けてもよいが、光ディスクの特定のエリアに書き込まれるようにしてもよい。この場合には、第８図に示すように、光ディスクの挿入（ステップ１０１）とともに、この光ディスクからエラープログラムを読み出してディスクドライブ装置内のエラー処理テーブルに格納し（１０８）、その後は第２図と同様の処理を行なつてエラー処理時（ステップ１０６）、このエラープログラムに従って上記の処理を行なうようにする。

〔発明の効果〕

以上説明したように、本発明によれば、記録媒体にユーザ固有情報を登録したユーザのみが該記録媒体のデータ再生が可能となり、データの秘密保護が確実に達成できる。

また、本発明によれば、記録媒体の正統なユーザ以外のユーザによる使用の痕跡を確実に残すことができ、記録データの信頼性が大幅に向上する。

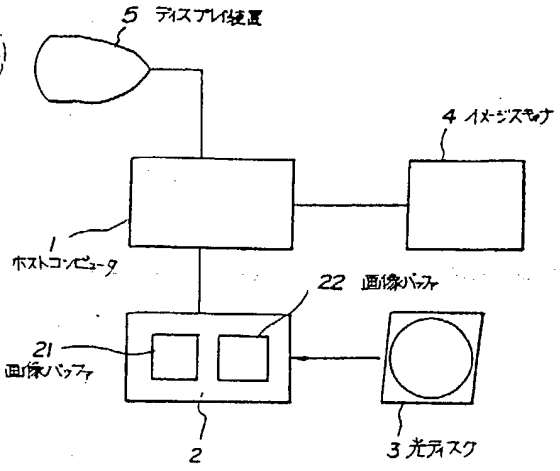
４．図面の簡単な説明

第１図は本発明によるデータ秘密保護方式の一実施例を示すブロック図、第２図はその動作を示すフローチャート、第３図は本発明によるデータ秘密保護方式の他の実施例でのデータ再生不能とする機能を説明するための図、第４図はデータ再生不能とされた記録媒体からのデータ再生可能手段の一具体例を示す図、第５図～第７図は本発明によるデータ秘密保護方式のさらに他の実施例でのデータ判別不能とするためのデータ変調方法を示す図、第８図はその動作を示すフローチャートである。

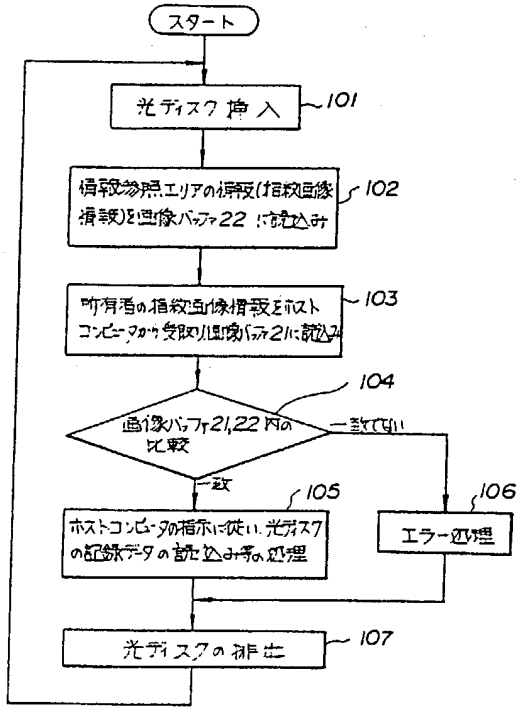
1……ホストコンピュータ、2……ディスクドライブ装置、21，22……画像バッファ、3……光ディスク、4……イメージスキャナ、5……ディスプレイ装置。

代理人　弁理士　武　顕次郎（外1名）

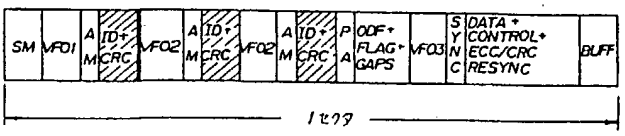
第1図



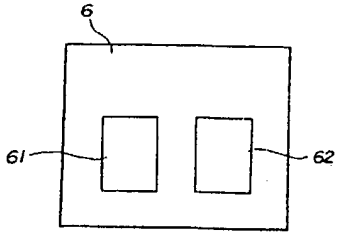
第2図



第3図



第4図



第 5 図

復調データ	変調データ
10	0100
010	100100
0010	00100100
11	1000
011	001000
0011	00001000
000	000100

第 6 図

エラー処理前	エラー処理後データ
0100	0110
100100	110110
00100100	00110110
1000	1100
001000	001100
00001000	00001100
000100	000110

第 7 図

復調データ	エラー処理後データ
10	0110
010	110110
0010	00110110
11	1100
011	001100
0011	00001100
000	000110

第 8 図